Приложение

УТВЕРЖДЕНА
к постановлению администрации
муниципального образования
Курганинский район
от 16.07.2026 г. № 801

ПОЛИТИКА
защиты информации, содержащейся в информационных системах администрации муниципального образования Курганинский район

1. Общие положения

1.1. Настоящая Политика защиты информации, содержащейся в информационных системах администрации муниципального образования Курганинский район (далее – Политика) разработана в соответствии с положениями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации, информационных технологиях и о защите информации), Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее - Требования о защите информации), приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет цели, стратегию, правила, методы и принципы защиты информационных активов администрации муниципального образования Курганинский район (далее – оператор) от угроз.

1.2. В рамках настоящей Политики под информационной системой понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.3. Оператор обеспечивает защиту информации на всех стадиях (этапах) обработки и хранения информации, создания и развития (модернизации), эксплуатации и вывода из эксплуатации информационной системы в рамках

функций, выполняемых им в соответствии с Законом об информации, информационных технологиях и о защите информации.

1.4. Действие настоящей Политики распространяется на всех работников, структурные подразделения, информационные системы, материальные и цифровые активы оператора, а также внешних пользователей, работающих с его данными.

Настоящая Политика обязательна для исполнения всеми подразделениями (работниками) оператора в части, их касающейся.

Организации, которым предоставляется доступ к информационным системам оператора и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации (далее - подрядные организации), должны быть ознакомлены с настоящей Политикой в части, их касающейся.

Обязанность подрядной организации по выполнению настоящей Политики должна быть определена в документах оператора, на основании которых в том числе передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.

1.5. Перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите, определен в приложении к настоящей Политике.

2. Цели и задачи защиты информации

2.1. Цели защиты информации определяются оператором исходя из ожидаемых результатов, направленных на недопущение или снижение негативных последствий от реализации угроз безопасности.

2.2. Основные цели защиты информации включают:

обеспечение защиты (некриптографическими методами) информации;

предотвращение несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, блокирования доступа к информации;

недопущение (снижение возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее - нарушение безопасности информации);

недопущение (снижение возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

2.3. Основными задачами защиты информации являются:

защита от несанкционированного доступа к информации, содержащейся в информационной системе;

предотвращение утечки информации;

мониторинг и обнаружение угроз;

создание безопасной цифровой среды.

3. Принципы защиты информации

3.1. Защита информации, содержащейся в информационной системе оператора, основывается на следующих принципах:

конфиденциальность: информация доступна только авторизованным пользователям, что создает защиту от утечек;

целостность: защита данных от случайного или намеренного изменения, подмены или удаления;

доступность: обеспечение бесперебойного доступа к информации авторизованных пользователей в нужное время;

законность и обоснованность защиты: защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством;

системность: необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления, во всех структурных элементах, при всех режимах функционирования;

комплектность: согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках ее компонентов;

непрерывность защиты: принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования;

разумная достаточность: стоимость защиты должна соответствовать потенциальному ущербу от потери данных;

персональная ответственность: каждый субъект доступа несет ответственность за свои действия.

4. Объекты защиты

4.1. Объектами защиты информации являются программные, программно-аппаратные средства, информационные системы, сети и подсети, образующие информационно-телекоммуникационную инфраструктуру оператора.

5. Организация и управление деятельностью по защите информации

5.1. Оператор организует деятельность по защите информации и управляет ею в соответствии с Требованиями о защите информации и настоящей Политикой.

5.2. Организация деятельности по защите информации включает:

разработку и утверждение настоящей Политики;

определение лиц, ответственных за защиту информации;

применение программных, программно-аппаратных средств, предназначенных для защиты информации;

разработку и утверждение внутренних стандартов по защите информации;

разработку и утверждение внутренних регламентов по защите информации;

выделение организационных, технических и иных ресурсов, необходимых для защиты информации.

5.3. Защиту информации организовывает руководитель оператора или по его решению ответственное лицо.

5.4. Обязанности (функции) и полномочия ответственного лица по организации деятельности по защите информации, управлению защитой информации, а также по организации контроля за данной деятельностью у оператора должны быть включены в должностные обязанности (трудовые функции) ответственного лица.

Состав обязанностей (функций) и полномочий ответственного лица должен быть достаточен для организации деятельности по защите информации и управления этой деятельностью в соответствии с Требованиями о защите информации и настоящей Политикой, а также организации контроля за данной деятельностью у оператора.

5.5. Руководитель оператора, ответственное лицо создают (определяют) структурное подразделение или назначают отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации (далее – структурное подразделение (специалисты) по защите информации).

Функции и полномочия по защите информации структурного подразделения по защите информации определяются в положении о структурном подразделении или ином документе, в соответствии с которым функционирует структурное подразделение.

Обязанности (функции) и полномочия специалистов по защите информации по проведению мероприятий и принятию мер по защите информации должны быть установлены в их должностных обязанностях (трудовых функциях).

Состав обязанностей (функций) и полномочий по защите информации структурного подразделения (специалистов) по защите информации должен быть достаточен для проведения мероприятий и принятия мер по защите информации в соответствии с Требованиями о защите информации и настоящей Политикой.

Примечание. В случае наличия у оператора структурного подразделения, на которое возложены функции по обеспечению информационной

безопасности, защита информации может быть возложена на указанное подразделение (пункт 19 Требований о защите информации).

5.6. Работники структурного подразделения (специалисты) по защите информации должны обладать компетенциями, необходимыми для выполнения возложенных на них обязанностей (функций) по защите информации в соответствии с Требованиями о защите информации и настоящей Политикой.

Не менее 30 процентов работников структурного подразделения по защите информации должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

5.7. Структурное подразделение (специалисты) по защите информации должно (должны) обеспечивать защиту информации во взаимодействии с подразделениями (работниками), использующими информационные системы, и подразделениями (работниками), обеспечивающими эксплуатацию информационных систем.

5.8. Подразделения (работники), использующие информационные системы, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном оператором во внутренних стандартах и регламентах по защите информации.

Подразделения, обеспечивающие эксплуатацию информационных систем, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания информационных систем, поставки комплектующих и иных видов работ по эксплуатации информационных систем в объеме, установленном оператором во внутренних стандартах и регламентах по защите информации.

5.9. Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечить выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

Состав программных, программно-аппаратных средств, необходимых структурному подразделению (специалистам) по защите информации для выполнения возложенных на них обязанностей (функций), определяется во внутренних стандартах и регламентах по защите информации.

5.10. Для проведения мероприятий и принятия мер по защите информации оператором могут привлекаться организации, имеющие лицензию

на деятельность по технической защите конфиденциальной информации (далее – специализированные организации).

Состав проводимых специализированными организациями мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется оператором.

Работники структурного подразделения (специалисты) по защите информации оператора должны привлекаться к приемке результатов работ и услуг, выполняемых (оказываемых) специализированными организациями.

5.11. Оператором разработаны и утверждены:

внутренние стандарты по защите информации, устанавливающие требования к реализации мер по защите информации применительно к особенностям деятельности оператора и функционирования информационных систем;

внутренние регламенты по защите информации, содержащие порядок проведения мероприятий или описание реализуемых процессов по защите информации применительно к особенностям деятельности оператора и функционирования информационных систем.

Область действия внутренних стандартов и регламентов по защите информации определена оператором.

5.12. Внутренние стандарты и регламенты по защите информации доводятся до пользователей, а также подрядных организаций в части, их касающейся.

Внутренние стандарты и регламенты по защите информации подлежат исполнению пользователями в части, их касающейся.

Обязанность подрядной организации по выполнению внутренних стандартов и регламентов по защите информации должна быть определена в документах оператора, на основании которых передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.

5.13. Структурное подразделение (специалисты) по защите информации должно (должны) разрабатывать и представлять руководителю оператора, ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов.

Руководитель оператора, ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации, привлечения при необходимости дополнительных сил и средств для защиты информации в соответствии с Требованиями о защите информации и

настоящей Политикой на всех этапах жизненного цикла информационных систем.

5.14. Управление деятельностью по защите информации осуществляется в рамках функционирующей организационной системы управления, возглавляемой руководителем оператора или по его решению ответственным лицом.

Управление деятельностью по защите информации включает:

разработку и планирование мероприятий и мер по защите информации;

проведение мероприятий и принятие мер по защите информации;

проведение оценки состояния защиты информации;

совершенствование мероприятий и мер по защите информации.

5.15. При разработке и планировании мероприятий и мер по защите информации должны быть:

определены события в информационных системах, наступление которых может привести к нарушению целей защиты информации, установленных в политике защиты информации;

определены информационные системы, программные, программно-аппаратные средства, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации, установленных в политике защиты информации;

выявлены и оценены угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению целей защиты информации, установленных в политике защиты информации (далее – угрозы безопасности информации);

определены состав и сроки проведения мероприятий и принятия мер по защите информации и оценены необходимые для этого ресурсы.

5.16. Проводимые мероприятия и принимаемые меры по защите информации должны быть направлены на блокирование (нейтрализацию) актуальных для информационной системы угроз безопасности информации (далее – актуальные угрозы) в соответствии с целями защиты информации, определенными в настоящей Политике.

В зависимости от целей защиты информации мероприятия и меры по защите информации должны быть направлены на:

исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

исключение или существенное затруднение отказа в обслуживании авторизованным пользователям информационных систем;

недопущение использования информационных систем и содержащейся в них информации не по назначению;

исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

недопущение распространения с использованием информационных систем противоправной информации;

обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки доступа авторизованных пользователей к информационным системам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

- обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

5.17. Оценка состояния защиты информации проводится на основе определения оператором:

показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее - показатель защищенности К зи);

показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации (далее - показатель уровня зрелости П зи).

Для определения значений и расчета показателя защищенности К зи и показателя уровня зрелости П зи применяются методические документы, утвержденные ФСТЭК России (далее - методические документы ФСТЭК России).

5.18. Расчет и оценка показателя защищенности К зи проводится оператором не реже одного раза в шесть месяцев.

Расчет и оценка показателя уровня зрелости П зи проводится оператором не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности К зи и показателя уровня зрелости П зи в случае их несоответствия нормированным значениям, указанным в методических документах ФСТЭК России, в течение 3 календарных дней со дня завершения такой оценки информируется руководитель оператора для принятия решения о проведении мероприятий по совершенствованию защиты информации и принятии мер по повышению уровня защищенности информации, содержащейся в информационных системах.

Результаты оценки показателя защищенности К зи и показателя уровня зрелости П зи направляются оператором в департамент информатизации и связи Краснодарского края в целях мониторинга текущего состояния технической защиты информации и оценки эффективности деятельности по технической защите информации.

5.19. По решению руководителя оператора, ответственного лица структурным подразделением (специалистами) по защите информации с участием подразделений (работников), использующих информационные системы, подразделений (работников), обеспечивающих эксплуатацию информационных систем, разрабатывается план мероприятий по совершенствованию защиты информации, содержащейся в информационных системах, в котором в том числе указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия.

План утверждается руководителем оператора, ответственным лицом и доводится до подразделений (работников) оператора в части, их касающейся.

Результатом реализации мероприятий плана должно быть достижение значений показателя защищенности К зи и показателя уровня зрелости П зи не ниже нормированных значений, указанных в методических документах ФСТЭК России.

6. Мероприятия и меры по защите информации

6.1. Для достижения целей защиты информации оператором проводятся следующие мероприятия:

выявление и оценка угроз безопасности информации;

контроль конфигураций информационных систем;

управление уязвимостями;

управление обновлениями;

обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;

обеспечение защиты информации при применении конечных устройств;

обеспечение защиты информации при применении мобильных устройств;

обеспечение защиты информации при удаленном доступе пользователей к информационным системам;

обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;

обеспечение защиты информации при предоставлении пользователям доступа к информационным системам, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в информационных системах (далее - привилегированный доступ);

обеспечение мониторинга информационной безопасности;

обеспечение разработки безопасного программного обеспечения;

обеспечение физической защиты информационных систем;

обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;

повышение уровня знаний и информированности пользователей по вопросам защиты информации;

обеспечение защиты информации при взаимодействии с подрядными организациями;

обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;

обеспечение защиты информации при использовании искусственного интеллекта;

реализация в информационных системах мер по их защите и защите содержащейся в них информации;

проведение контроля уровня защищенности информации, содержащейся в информационных системах;

обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

6.2. Достаточность и эффективность проводимых мероприятий (реализованных процессов) оцениваются оператором по результатам определения показателя уровня зрелости П зи в соответствии с пунктами 5.18 и 5.19 настоящей Политики.

6.3. Мероприятия по выявлению и оценке угроз безопасности информации предусматривают определение в ходе создания информационных систем актуальных угроз и разработку в случаях, установленных требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676, моделей угроз безопасности информации, а также своевременное выявление актуальных угроз и их оценку в ходе эксплуатации информационных систем.

Модель угроз безопасности информации в случае ее разработки используется в качестве исходных данных для разработки и внедрения мер по защите информации, а также для выбора средств защиты информации и их функциональных возможностей в ходе создания (развития) подсистем защиты информации информационных систем. Решение о необходимости разработки модели угроз безопасности информации в ходе создания негосударственных информационных систем принимается руководителем оператора (обладателя информации), ответственным лицом.

В ходе эксплуатации информационных систем обеспечивается поиск данных и признаков, идентифицирующих наличие актуальных угроз, проведена приоритизация выявленных угроз безопасности информации, осуществлено оповещение подразделений (работников) оператора (обладателя информации) о выявленных актуальных угрозах. При наличии признаков реализации

(возникновения) актуальных угроз должны быть приняты меры по их блокированию (нейтрализации).

6.4. Мероприятия по контролю конфигураций информационных систем исключают несанкционированное изменение состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечивать обнаружение фактов несанкционированных изменений и выявление причин изменений.

Контроль конфигураций информационных систем осуществляется на основе анализа результатов учета ИТ-активов и (или) сведений, содержащихся в автоматизированных системах хранения и управления данными об информационных системах и их конфигурациях (при наличии систем инвентаризации ИТ-активов).

Структурному подразделению (специалистам) по защите информации должен быть обеспечен доступ к указанным сведениям.

6.5. Мероприятия по управлению уязвимостями включают выявление уязвимостей информационных систем, оценку их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

Устранение уязвимостей, которые могут быть использованы нарушителями, или исключение возможности их использования за счет применения компенсирующих мер проводится оператором:

в отношении уязвимостей критического уровня опасности - в срок не более 24 часов;

в отношении уязвимостей высокого уровня опасности - в срок не более 7 календарных дней.

В отношении уязвимостей среднего и низкого уровней опасности сроки и порядок их устранения определяются во внутреннем регламенте по защите информации исходя из особенностей функционирования информационных систем.

При выявлении уязвимостей информационных систем, сведения о которых отсутствуют в банке данных угроз безопасности информации ФСТЭК России, оператор в срок не более 5 рабочих дней с даты такого выявления направляет информацию об уязвимости в ФСТЭК России для оценки необходимости включения выявленной уязвимости в банк данных угроз безопасности информации ФСТЭК России.

6.6. Мероприятия по управлению обновлениями включают проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестирования обновлений до их применения в контурах промышленной эксплуатации информационных систем, выдачу разрешения подразделениям (работникам) оператора на применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации информационных систем с использованием безопасных настроек

и конфигураций, установленных во внутренних стандартах по защите информации.

Бесконтрольная установка обновлений программных, программно-аппаратных средств не допускается.

Сроки применения обновлений программных, программно-аппаратных средств, предназначенных для устранения уязвимостей, устанавливаются во внутреннем регламенте по защите информации в зависимости от сроков устранения уязвимостей соответствующих уровней опасности и рисков, связанных с применением обновлений программных, программно-аппаратных средств.

6.7. Мероприятия по защите информации при обработке, хранении и обращении с информацией ограниченного доступа должны исключать:

неправомерное распространение информации ограниченного доступа вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети "Интернет";

доступ к информации ограниченного доступа лиц, для которых информация не предназначена и (или) для которых такой доступ запрещен.

Проводимые мероприятия включают определение информации ограниченного доступа и предназначенных для ее хранения программно-аппаратных средств, а также контроль и регистрацию всех фактов доступа пользователей к программно-аппаратным средствам, в которых хранится информация ограниченного доступа.

Контроль обработки, хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи осуществляется в соответствии с внутренним регламентом по защите информации.

О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам ее обработки и хранения незамедлительно информируется руководитель оператора, ответственное лицо.

6.8. Мероприятия по обеспечению защиты информации при применении конечных устройств информационных систем исключают возможность несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью "Интернет" и (или) доступные из сети "Интернет".

Защита конечных устройств информационных систем включает реализацию в них мер по защите информации от несанкционированного доступа и проведению на них мониторинга и анализа процессов и событий с целью выявления актуальных угроз, а также предупреждении о произошедших событиях безопасности.

Контроль использования конечных устройств осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.9. Посредством проведения мероприятий по обеспечению защиты информации при применении мобильных устройств исключается возможность

несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними мобильным устройствам и содержащейся в них информации через каналы передачи мобильных данных, мобильные сервисы, интерфейсы и порты мобильных устройств.

При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператор принимает меры по защите информационных систем и содержащейся в них информации, в том числе:

обеспечивает защиту каналов передачи данных;

осуществляет доступ пользователей с применением строгой аутентификации.

Пользователем должен быть исключен несанкционированный доступ к мобильному устройству.

6.10. Применение пользователями личных мобильных устройств для доступа к информационным системам и содержащейся в них информации с целью выполнения своих обязанностей (функций) допускается в случае соответствия мобильных устройств Требованиям о защите информации и наличия у оператора возможности контроля использования мобильных устройств.

6.11. Контроль использования мобильных устройств осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.12. При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации, не связанного с выполнением пользователем своих обязанностей (функций), в том числе для доступа к общедоступной информации, оператором принимаются меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечивается защита каналов передачи данных, используемых для осуществления доступа.

6.13. Посредством проведения мероприятий по обеспечению защиты информации при удаленном доступе пользователей исключается возможность несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними программно-аппаратным средствам пользователей через каналы передачи данных, интерфейсы и порты удаленно подключаемых программно-аппаратных средств.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором принимаются меры по защите информационных систем и содержащейся в них информации, обеспечивается защита каналов передачи данных и программно-аппаратных средств, с использованием которых

осуществляется удаленный доступ, исключается несанкционированный доступ к удаленно подключаемому программно-аппаратному средству пользователя.

Удаленный доступ пользователей в целях выполнения своих обязанностей (функций) осуществляется с использованием программно-аппаратных средств, выделенных оператором и соответствующих Требованиям о защите информации. По согласованию со структурным подразделением (специалистами) по защите информации допускается предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств пользователя оператора при условии применения для удаленного доступа сертифицированных средств обеспечения безопасной дистанционной работы, средств антивирусной защиты и иных средств защиты информации, исключающих угрозы безопасности информации, связанные с удаленным доступом.

Удаленный доступ пользователей к информационным системам в целях выполнения своих обязанностей (функций) осуществляется с использованием сетей связи, расположенных на территории Российской Федерации, посредством применения средств защиты канала передачи данных, и строгой аутентификации пользователей.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации, не связанном с выполнением пользователями своих обязанностей (функций), в том числе при доступе к общедоступной информации, оператором принимаются меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечивается защита каналов передачи данных, используемых для осуществления удаленного доступа.

Контроль удаленного доступа пользователей к информационным системам осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.14. Посредством проведения мероприятий по обеспечению защиты информации при беспроводном доступе пользователей к информационным системам исключается возможность несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации за счет несанкционированного подключения к точкам беспроводного доступа и доступа к беспроводным каналам передачи данных, подмены взаимодействующих с ними программно-аппаратных средств или доступа к ним.

При беспроводном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором принимаются меры по защите информационных систем и содержащейся в них информации, обеспечивается защита беспроводных каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется беспроводной доступ. Посредством формирования конфигурации и настроек, уровней сигналов точек беспроводного доступа, используемых для подключения пользователей к информационным системам в

целях выполнения своих обязанностей (функций), исключается возможность подключения к ним лиц, не имеющих прав доступа к информационным системам. Указанные точки беспроводного доступа должны быть однозначно идентифицированы в информационных системах, а также определены места их размещения.

Точки беспроводного доступа и построенные на их основе беспроводные сети связи, используемые для доступа пользователей к информационным системам и содержащейся в них информации в целях выполнения ими своих обязанностей (функций), должны быть изолированы от беспроводных сетей связи, предназначенных для доступа к сети "Интернет" и (или) общедоступной информации оператора (обладателя информации).

6.15. Посредством проведения мероприятий по обеспечению защиты информации при предоставлении привилегированного доступа исключается возможность получения привилегированного доступа к информационным системам лицами, для которых такой доступ должен быть исключен, а также использования повышенных прав доступа с нарушением внутренних стандартов и регламентов по защите информации.

Для получения привилегированного доступа создаются привилегированные учетные записи. Привилегированные учетные записи должны иметь права доступа, минимально необходимые для выполнения пользователями возложенных на них обязанностей (функций), в соответствии с принятыми в информационных системах моделями доступа пользователей. Привилегированные учетные записи, имеющие права по созданию других привилегированных учетных записей, должны быть персонифицированными.

Привилегированный доступ осуществляется с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации - с использованием усиленной многофакторной аутентификации.

Не допускается объединение в рамках одной привилегированной учетной записи или одной группы привилегированных учетных записей ролей по системному администрированию, ролей по разработке и тестированию программных, программно-аппаратных средств, ролей администраторов безопасности.

Неиспользуемые привилегированные учетные записи должны быть заблокированы и удалены в соответствии с внутренними стандартами и регламентами по защите информации.

Встроенные привилегированные учетные записи должны быть отключены или, в случае невозможности отключения, переименованы после завершения настройки и установки конфигураций, заданных внутренними стандартами по защите информации. Аутентификационная информация встроенных привилегированных учетных записей должна быть изменена в соответствии с внутренними стандартами и регламентами по защите информации.

Все действия по доступу пользователей с использованием привилегированных учетных записей подлежат регистрации. Контроль использования привилегированных учетных записей осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.16. Мероприятия по осуществлению мониторинга информационной безопасности предусматривают сбор данных о событиях безопасности, их обработке и анализе, а также выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации. Мероприятия по осуществлению мониторинга информационной безопасности проводятся в отношении всех информационных систем, за исключением локальных и изолированных информационных систем, в которых должен обеспечиваться контроль журналов регистрации событий безопасности.

Мероприятия по мониторингу информационной безопасности осуществляются в соответствии с разделами 4 и 5 ГОСТ Р 59547-2021.

В ходе проведения мониторинга информационной безопасности для анализа зафиксированных событий безопасности и выявленных в них признаков реализации актуальных угроз допускается использование доверенных технологий искусственного интеллекта.

Структурное подразделение (специалисты) по защите информации оператора с периодичностью и в сроки, установленные внутренним регламентом по защите информации, разрабатывает и представляет руководителю оператора, ответственному лицу отчет о результатах мониторинга, который в том числе должен содержать типы событий безопасности, обнаруженные по результатам мониторинга, и связанные с ними компьютерные инциденты (при их наличии), а также рекомендации по их анализу и (или) устранению. Последний в текущем году отчет о результатах мониторинга или итоговый отчет за текущий год (в случае его разработки) после представления руководителю оператора направляется оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации.

6.17. Мероприятия по разработке безопасного программного обеспечения направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом оператором программном обеспечении. Мероприятия по разработке безопасного программного обеспечения проводятся в случае осуществления оператором самостоятельной разработки программного обеспечения, применяемого в информационных системах.

В случае самостоятельной разработки оператором программного обеспечения, предназначенного для использования в информационных системах, реализуются меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.

В случае привлечения оператором для разработки программного обеспечения подрядной организации по решению руководителя

(ответственного лица) в техническое задание на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024.

6.18. Посредством проведения мероприятий по обеспечению физической защиты информационных систем исключается возможность несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации.

Физический доступ к программно-аппаратным средствам информационных систем, предназначенным для обработки и хранения информации, предоставляется пользователям, которым указанный доступ необходим для выполнения возложенных на них обязанностей (функций). Программно-аппаратные средства информационных систем, предназначенные для хранения информации, должны быть установлены в помещениях (зонах помещений, шкафах, футлярах, корпусах), несанкционированный физический доступ в которые должен быть исключен.

Контроль физического доступа к программно-аппаратным средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений, шкафы, футляры, корпуса), в которых они установлены, осуществляется в соответствии с внутренними регламентами по защите информации.

Съемные машинные носители информации подлежат контролю использования. В случае обнаружения пользователем съемного машинного носителя информации, принадлежность которого или владельца которого установить не удалось, такой съемный машинный носитель информации должен быть передан в структурное подразделение (специалистам) по защите информации для анализа содержащейся на нем информации, программ и при необходимости дальнейшего уничтожения. Подключение обнаруженного съемного машинного носителя информации к информационным системам запрещается.

6.19. Посредством проведения мероприятий по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций обеспечивается возможность восстановления выполнения функций (процессов, видов работ) информационных систем, для которых оператором установлены требования к непрерывному режиму функционирования (далее - значимые функции), в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

6.20. Интервалы времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции, устанавливаются оператором в соответствии с актами, на основании которых осуществляется создание, эксплуатация информационных систем, или требованиями обладателя информации в зависимости от значимости функций для обеспечения его деятельности, классов защищенности информационных

систем, устанавливаемых оператором в соответствии с приложением к Требованиям о защите информации, и должны составлять:

для информационных систем 1 класса защищенности - не более 24 часов с момента обнаружения нарушения функционирования;

для информационных систем 2 класса защищенности - не более 7 календарных дней с момента обнаружения нарушения функционирования;

для информационных систем 3 класса защищенности - не более 4 недель с момента обнаружения нарушения функционирования.

6.21. Программные, программно-аппаратные средства, позволяющие обеспечить выполнение значимых функций, должны быть развернуты в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный оператором во внутренних стандартах и регламентах по защите информации интервал времени восстановления.

6.22. Оператором обеспечивается:

создание достаточного количества резервных копий программных, программно-аппаратных средств и их конфигураций, обеспечивающих выполнение значимых функций, необходимых для восстановления выполнения значимых функций в установленный во внутренних стандартах и регламентах по защите информации интервал времени восстановления, и периодическое тестирование таких средств на работоспособность;

создание достаточного количества резервных копий информации, необходимой для обеспечения выполнения значимых функций, а также их хранение на разных типах машинных носителей информации в местах, обеспечивающих исключение несанкционированного доступа к резервным копиям информации.

Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации определяются во внутренних стандартах и регламентах по защите информации.

Оператор проводит периодические, но не реже одного раза в два года, проверки, в том числе в форме тренировок, возможности восстановления выполнения значимых функций с использованием резервных копий программных, программно-аппаратных средств и информации, необходимой для их выполнения, с привлечением работников, задействованных в проведении работ по восстановлению функционирования информационных систем.

В случае проведения мероприятий по восстановлению функционирования информационных систем, их сегментов, выполняющих значимые функции, с превышением интервалов времени их восстановления должна обеспечиваться возможность выполнения пользователями значимых функций, в том числе в неавтоматизированном режиме, в соответствии с внутренними регламентами по защите информации.

6.23. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации включают:

доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

проведение лекций и семинаров по вопросам защиты информации;

проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;

проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

6.24. Применяемые оператором способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний определяются во внутренних регламентах по защите информации. Оценка уровня знаний проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора. Для пользователей, у которых отсутствуют знания по вопросам защиты информации, организуется повторное прохождение обучающих курсов по вопросам защиты информации.

6.25. Посредством проведения мероприятий по защите информации при взаимодействии оператора с подрядными организациями исключается возможность несанкционированного доступа или воздействий на информационные системы и содержащуюся в них информацию через взаимодействующие с информационными системами программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы, используемые для доступа подрядных организаций к информационным системам.

Оператором в отношении подрядной организации устанавливаются требования по обеспечению защиты информации, к которой получен доступ.

Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в документах оператора, на основании которых подрядным организациям предоставлен доступ к информационным системам.

В информационных системах, отдельных программно-аппаратных средствах подрядных организаций, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации. Состав информации, цели ее защиты и классы защищенности, в соответствии с которыми подрядными организациями должны быть приняты меры по защите информации во

взаимодействующих информационных системах, устанавливаются оператором во внутренних стандартах и регламентах по защите информации.

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в эксплуатируемых информационных системах оператора не допускается. Для проведения работ по разработке (развитию) и (или) тестированию программного обеспечения работникам подрядных организаций предоставляется доступ к выделенным для проведения таких работ стендам разработки и (или) тестирования, которые должны быть изолированы от эксплуатируемых информационных систем оператора. Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования осуществляется в соответствии с внутренними регламентами по защите информации.

6.26. Посредством проведения мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании, исключается возможность блокирования авторизованным пользователям доступа к информационным системам и (или) содержащейся в них информации вследствие несанкционированных воздействий на интерфейсы, порты, сервисы, к которым должен быть обеспечен постоянный доступ из сети "Интернет".

Обеспечение доступности из сети "Интернет" интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, осуществляется в соответствии с внутренними регламентами по защите информации по согласованию со структурным подразделением (специалистами) по защите информации после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с перечнем ресурсов сети "Интернет", с которыми может взаимодействовать информационная система, включающим исходящий и входящий сетевые потоки, их характеристики и используемые протоколы.

6.27. Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта обеспечивается возможность исключения несанкционированного доступа к информации или воздействия на информационные системы, несанкционированного распространения и модификации информации, а также использования информационных систем не по их назначению за счет воздействия на наборы данных, применяемые модели искусственного интеллекта и их параметры, процессы и сервисы по обработке данных и поиску решений.

Не допускается передача лицу, разработавшему модель искусственного интеллекта, информации ограниченного доступа, содержащейся в информационных системах, в том числе для улучшения функционирования модели искусственного интеллекта.

6.28. При взаимодействии пользователей в целях выполнения ими своих обязанностей (функций) с сервисами на основе искусственного интеллекта посредством направления запроса и получения ответа должны быть:

при взаимодействии в формате строго заданных шаблонов запросов и ответов:

определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам;

определены шаблоны ответов искусственного интеллекта и обеспечен контроль соответствия ответов установленным оператором шаблонам;

при взаимодействии в формате свободной текстовой формы запросов и ответов:

определены для направляемых в искусственный интеллект запросов пользователей допустимые тематики и обеспечен контроль соответствия запросов допустимым тематикам;

определены форматы ответов искусственного интеллекта в соответствии с допустимыми тематиками и обеспечен контроль соответствия ответов установленным оператором форматам и допустимым тематикам;

разработаны статистические критерии для выявления недостоверных ответов искусственного интеллекта для последующего сбора и анализа недостоверных ответов;

обеспечено реагирование на недостоверные ответы искусственного интеллекта посредством ограничения области принимаемых решений и (или) реализации функций информационной системы на основе недостоверных ответов искусственного интеллекта.

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование информационных систем.

Непосредственно в состав информационных систем должны включаться доверенные технологии искусственного интеллекта или их компоненты.

6.29. Мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации включают:

реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором;

адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

6.30. В информационных системах реализованы следующие базовые меры защиты информационных систем и содержащейся в них информации:

идентификация и аутентификация;

управление доступом;
регистрация событий безопасности;
защита сервисов электронной почты;
защита веб-технологий;
защита программных интерфейсов взаимодействия приложений;
защита конечных устройств;
антивирусная защита;
обнаружение и предотвращение вторжений на сетевом уровне;
сегментация и межсетевое экранирование;
защита от компьютерных атак, направленных на отказ в обслуживании;
защита каналов передачи данных и сетевого взаимодействия.

6.31. Реализация мер по защите информационных систем и содержащейся в них информации, подлежащие реализации, обеспечивает защиту от нарушителей со следующими уровнями возможностей:

в информационных системах 3 класса защищенности - от нарушителей с базовым уровнем возможностей;

в информационных системах 2 класса защищенности - от нарушителей с повышенным уровнем возможностей;

в информационных системах 1 класса защищенности - от нарушителей с высоким уровнем возможностей.

Оператором может быть принято решение о применении мер защиты информационных систем и содержащейся в них информации от нарушителей с более высоким уровнем возможностей.

6.32. С целью подтверждения достаточности принятых мер защиты информационных систем и содержащейся в них информации до начала обработки и (или) хранения информации в информационных системах может быть проведена их аттестация на соответствие Требованиям о защите информации.

Решение о необходимости аттестации информационных систем принимается руководителем оператора, ответственным лицом.

6.33. Мероприятия по контролю уровня защищенности информации, содержащейся в информационных системах, обеспечивают включение проведения оценки возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями.

Контроль уровня защищенности информации проводится в соответствии с внутренними регламентами по защите информации одним или совокупностью следующих методов:

автоматизированное и (или) ручное выявление уязвимостей информационных систем с последующей экспертной оценкой возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования информационных систем;

выявление несанкционированных подключений устройств к информационным системам;

тестирование информационных систем путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ним (воздействий на них) или повышения привилегий при реализованных мероприятиях и мерах по защите информационных систем и содержащейся в них информации;

проведение в соответствии с планом тренировок по отработке работниками оператора действий по обеспечению уровня защищенности информации, содержащейся в информационных системах, в условиях реализации актуальных угроз.

6.34. Контроль уровня защищенности информации проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора. Методы контроля уровня защищенности информации и периодичность его проведения определяются оператором во внутреннем регламенте.

По результатам проведения контроля уровня защищенности информации разрабатывается отчет, который подписывается лицами, проводившими контроль. Отчет должен быть представлен в течение 3 рабочих дней с даты завершения контроля уровня защищенности информации руководителю оператора, ответственному лицу для принятия при необходимости решения руководителя оператора о выделении ресурсов с целью повышения уровня защищенности информации. Отчет направляется оператором в департамент информатизации и связи Краснодарского края в целях мониторинга текущего состояния технической защиты информации.

6.35. Мероприятия и меры по защите информации, предусмотренные Требованиями о защите информации и настоящей Политикой, реализуются оператором с использованием методических документов ФСТЭК России.

6.36. При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации оператором разрабатываются и внедряются компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных угроз. При этом оператором должно быть обосновано применение компенсирующих мер на этапе создания информационных систем, а при аттестации информационных систем - подтверждена их эффективность для блокирования (нейтрализации) актуальных угроз.

6.37. Технические меры по защите информации принимаются на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре при ее наличии. На аппаратном и системном уровнях защита информации обеспечивается посредством применения встроенных в аппаратное обеспечение и системное программное обеспечение средств защиты информации. На прикладном и сетевом (инфраструктурном) уровнях защита информации обеспечивается применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.

6.38. Для защиты информации применяются сертифицированные средства защиты информации в соответствии с инструкциями (правилами) по их эксплуатации, установленными разработчиками в эксплуатационной документации. Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

Средства защиты информации применяются с соблюдением запретов, установленных пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

6.39. Применяемые сертифицированные средства защиты информации должны соответствовать:

для защиты информационных систем 1 класса защищенности - не ниже чем 4 классу защиты и уровню доверия;

для защиты информационных систем 2 класса защищенности - не ниже чем 5 классу защиты и уровню доверия;

для защиты информационных систем 3 класса защищенности - 6 классу защиты и уровню доверия.

6.40. На стадиях жизненного цикла информационных систем меры по защите информации принимаются оператором в соответствии с разделом 5 национального стандарта Российской Федерации ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования», утвержденного и введенного в действие приказом Росстандарта от 28 января 2014 г. № 3-ст.

7. Обработка информации, содержащей персональные данные

7.1. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных» (далее - Закон о персональных данных).

7.2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

7.3. Оператор обеспечивает безопасность персональных данных при их обработке в информационной системе.

7.4. Оператор осуществляет выбор средств защиты информации для системы защиты персональных данных в соответствии с нормативными

правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

7.5. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7.6. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда.

7.7. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

7.8. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.9. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных

данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.10. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.11. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.12. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

обеспечение сохранности носителей персональных данных;

утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

7.13. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 7.12 настоящей Политики, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

7.14. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 7.13 настоящей Политики, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

7.15. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 7.14 настоящей Политики, необходимо выполнение следующих требований:

автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо

возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

7.16. Контроль за выполнением указанных в настоящем разделе требований организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором.

8. Ответственность

8.1. Нарушение требований Закона об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Исполняющий обязанности
начальника отдела информатизации
администрации муниципального
образования Курганинский район В.В. Назаров